Distributed Security Architectures

Fourth Quarter 2002 Progress Report

Covers work done July through Sept, 2002

Personnel:

Staff: Mary Thompson, Abdelilah Essiari, Keith Beattie

Students: Jiewei Lin, Maria Kulik

Akenti Server interfaces

Added a C compatible interface to the Akenti Client to return unconditional actions. This was needed by the new Globus job-manager which is using system attributes to support access control based on RSL parameters specifying resource requirements.

Akenti Policy Engine

Instrumented the policy engine with additional logging statements in order to do fine-grained performance measurements. Our measurements showed that about 60-70% of the time in the policy engine was spent in fetching certificates. The next largest percent of time was 5-7% in certificate validation. Several frequently used methods: smart pointer and base64 encoding, were optimized as a result of these measurements. The approximate time for an access check on a 450MH linux platform, for a case that requires 8 certificates and has no certificate caching was 230 milliseconds. This compares to the Akenti 1.0 number of 2.26 seconds on a 180MH Solaris machine.

With certificate caching on (and all the certificates found in the cache) the time dropped to 5.9 milliseconds. The comparable Akenti 1.0 number was 115 milliseconds. These numbers show an improvement somewhere around a factor of ten in the performance of the code. A paper presenting these measurement was submitted to a special edition of the ACM Transactions on Information and System Security and is available at http://www-itg.lbl.gov/Akenti/Papers/ACMTISSEC.pdf.

Progress was made on compiling the code with the g++3 compiler. This version of the compiler is more rigorous about enforcing name space usage. We also had to change our code to comply with some changes in throwable classes and vector templates. Approximately 3/4 of the code now compiles with g++3.

Certificate Generators

Continued to add support for Policy Certificate generation in the absence of any hint files. Now any field can be entered manually as well as selecting pre-loaded values from existing hint files or policy certificates.

Worked on making the connection between the generators and the Resource Definition server through https. We have finished the server side, but are still working on the client side. The motivation for this change is to allow newly created certificates to be uploaded securely to the resource server machine.

Code Distribution

Modified the client interface code to facilitate its use by the Globus job-manager. Continued to update our distribution files to represent the latest code changes.

Updated the Apache/ssl/akenti Web server to Apache version 1.3.26 to keep current with the Apache security patches.

Collaboration with the Secure and Reliable Group Communication and Peer2Peer Information Sharing project

Design and implementation was started on a C++ security library. This library will facilitate sharing of high quality implementations of commonly used security functions among these two projects and Akenti. This library will start with code developed for Akenti that provides C++ objects to handle SSL sockets, wraps OpenSSL and X.509 certificate structures and methods, as well as providing some more generic utility classes. This library should leverage the experience and expertise of the Akenti C++ coders to other projects in the department.